BENJAMIN C. MIZER
Acting Assistant Attorney General
JONATHAN F. OLIN
Deputy Assistant Attorney General
MICHAEL S. BLUME
Director, Consumer Protection Branch
RICHARD GOLDBERG
Assistant Director, Consumer Protection Branch
JOHN W. BURKE
Trial Attorney, Consumer Protection Branch
U.S. Department of Justice
450 Fifth Street, NW, Suite 6400 South
Washington, D.C. 20001
Telephone: (202) 353-2001
Facsimile: (202) 514-8742
E-mail: Josh.Burke@usdoj.gov

STEPHANIE K. YONEKURA
Acting United States Attorney
LEON W. WEIDMAN
Chief, Civil Division
ANOIEL KHORSHID
Assistant United States Attorney (California Bar #223912)
300 N. Los Angeles Street, Suite 7516
Los Angeles, California 90012
Telephone: (213) 894-6086
Facsimile: (213) 894-7819
Email: Anoiel.Khorshid@usdoj.gov

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. COMMERCEWEST BANK, Defendant.	No.: CV 15-00379 COMPLAINT FOR CIVIL PENALTIES, PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF [12 U.S.C. § 1833a, 18 U.S.C. § 1345]

Plaintiff, the United States of America, by its undersigned attorneys, alleges as follows:

1. This is an action for injunctive relief and civil penalties by the United States of America against CommerceWest Bank ("CWB" or "the Bank").

2. CWB – knowingly or with deliberate ignorance – allowed one of its clients to facilitate the theft of tens of millions of dollars from the bank accounts of unsuspecting, innocent consumers. Over the course of more than a year, CWB ignored a series of glaring red flags, including but not limited to return rates exceeding fifty percent, thousands of complaints from consumers, and even multiple complaints from other banks whose customers had been victims of these fraud schemes. By the time the Department of Justice became aware of this illegal activity and forced CWB to stop it, the Bank had permitted hundreds of thousands of unauthorized charges from consumer bank accounts.

I.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 (federal question) and 28 U.S.C. § 1345 (United States as plaintiff).

4. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391(b) because defendant CWB operates and maintains its management offices and its operations center in this district, and a substantial part of the events or omissions giving rise to the claims alleged in this complaint occurred in this district.

II.

PARTIES

5. Plaintiff is the United States of America.

6. Defendant CommerceWest Bank is a federally-insured commercial bank established in 2001 under the laws of California.

7. CWB maintains its principal executive office at 2111 Business Center Drive in Irvine, California. In addition to its headquarters, CWB has three regional offices in California, located in Newport Beach, Gardena, and San Marcos.

8. As of December 31, 2014, CWB had total assets of approximately $422 million.

9. CWB is regulated by the Federal Reserve Bank of San Francisco and the California Department of Business Oversight.

III.

RELEVANT STATUTES

A. The Financial Institutions Reform, Recovery And Enforcement Act.

10. The United States seeks civil money penalties from CWB under the Financial Institutions Reform, Recovery and Enforcement Act, 12 U.S.C. § 1833a ("FIRREA"), which Congress enacted as part of a comprehensive legislative plan to reform and strengthen the banking system and the federal deposit insurance system that protects the public from bank failures. Toward that end, FIRREA authorizes civil enforcement for violations of enumerated, predicate federal criminal offenses, including wire fraud affecting a federally-insured financial institution. CWB's actions affected dozens of federally-insured financial institutions whose customers were defrauded as a result of CWB's actions. In addition, CWB itself was and is a federally-insured financial institution and was affected by its unlawful conduct. See, e.g., United States v. Bank of New York Mellon, 941 F. Supp. 2d 438, 461-63 (S.D.N.Y. 2013); United States v. Countrywide Fin. Corp., 961 F. Supp. 2d 598, 606 (S.D.N.Y. 2013); United States v. Wells Fargo Bank, N.A., 972 F. Supp. 2d 593, 630 (S.D.N.Y. 2013).

11. FIRREA's penalty provisions provide that the United States may recover civil money penalties of up to $1.1 million per violation, or for a continuing violation, up to $1.1 million per day or $5.5 million, whichever is less. See 12 U.S.C. §§ 1833a(b)(1), (2); 28 C.F.R. § 85.3. The statute further provides that the

penalty can exceed these limits to permit the United States to recover the amount of any gain to the person committing the violation, or the amount of the loss to a person other than the violator stemming from such conduct, up to the amount of the gain or loss. See 12 U.S.C. § 1833a(b)(3).

B. The Anti-Fraud Injunction Act.

12. The United States seeks statutory equitable relief under Title 18, United States Code, Section 1345 ("Section 1345"). Section 1345 authorizes the government to commence a civil action to enjoin enumerated, predicate federal criminal offenses, including wire fraud.

13. Wire fraud is committed by sending a "wire . . . in interstate or foreign commerce" for the purpose of executing, or attempting to execute, "[a] scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises." 18 U.S.C. § 1343.

IV.

CONSUMER FRAUD IN THE 21ST CENTURY: HOW FRAUDULENT MERCHANTS ACCESS THE ELECTRONIC BANKING SYSTEM AND STEAL MONEY FROM UNSUSPECTING CONSUMERS

A. Federal Law Requires Banks To Know Their Customers.

14. Federal law requires CWB, like all banks in the United States, to have an effective program in place to assure that the Bank knows the identities of its customers and understands the nature of its customers' business activities, as well as to prevent illegal use of the banking system by the Bank's customers. See generally Bank Secrecy Act, 31 U.S.C. § 5311 et seq.; USA Patriot Act, § 326; 31 U.S.C. § 5318; 31 C.F.R. § 1020 et seq. (formerly 31 C.F.R. § 103 et seq.). Such programs are designed to prevent banks from providing access to the national banking system to entities engaged in unlawful activity.

15. During the relevant time period of its misconduct, CWB was required to conduct meaningful due diligence investigations of new clients at the

time of a new account opening. See 31 C.F.R. § 103.121 (amended 31 C.F.R. § 1020, et seq.).

16. In conducting a meaningful "know-your-customer" analysis, CWB was required to collect information sufficient for the Bank to determine whether a client poses a threat of criminal or other improper conduct.

17. Because of such requirements, many fraudulent merchants have difficulty obtaining bank accounts from which they can access the national banking system.

B. The Relationship Between Third-Party Payment Processors, Banks, And Consumers.

18. Third-party payment processors are intermediaries between banks and merchants. Third-party payment processors open bank accounts in their own names and use these accounts to conduct banking activities on behalf of their merchant-clients. Typically, the merchant-client does not have a direct relationship with the bank when a third-party payment processor is involved. Rather, the bank interacts with the third-party payment processor, which in turn interacts with the merchant.

19. Customers of third-party payment processors often are legitimate businesses. In some cases, however, customers of third-party payment processors are fraudulent merchants that do not or cannot open their own bank accounts because banks will not do direct business with them. Thus, these fraudulent merchants must rely on third-party payment processors to access the nation's banking system. At the merchants' direction, the processor will initiate debit transactions against consumers' accounts through its banking account and transmit the consumers' money to the fraudulent merchant.

20. Given the strict rules in place requiring banks to know their customers and have an effective Bank Secrecy Act/Anti-Money Laundering compliance program, bank regulators have warned banks about the risks associated

with providing certain banking services to third-party payment processors (and by proxy their merchant-clients).

21. As early as 2008, bank regulators have urged banks to ensure that they are not abetting consumer fraud by taking particular precautions when dealing with payment processor customers. These steps have included:

a. monitoring all transaction returns (unauthorized returns and total returns);

b. reviewing the third-party payment processor's promotional materials to determine its target clientele;

c. determining whether the third-party payment processor re-sells its services to other entities;

d. reviewing the third-party payment processor's policies and procedures to determine adequacy of merchant due diligence;

e. reviewing main lines of business and return volumes for the third-party payment processor's merchants; and

f. requiring that the third-party payment processor provide the bank with information about its merchants to enable the bank to assure that the merchants are operating lawful businesses.

C. Fraudulent Merchants Working With Third-Party Payment Processors Can Exploit Advances In Banking Technology To Harm Consumers.

22. Most consumers are familiar with the typical process for paying for items by check: the consumer (the "payor") signs a check from his or her bank and delivers it to the merchant (the "payee"). The merchant deposits the check in the merchant's bank, and the merchant's bank then withdraws funds from the bank of the consumer.

23. A demand draft (also referred to as a remotely-created check ("RCC") and/or a remotely-created payment order ("RCPO")) is a check created not by the account holder but rather by a third party using the account holder's name and

bank account information. Unlike ordinary checks, demand drafts are not signed by the account holder. In place of the account holder's signature, a demand draft contains a statement claiming that the account holder has authorized the check. For example, many demand drafts, including those deposited at CWB, included a legend stating "NO SIGNATURE REQUIRED. This payment has been authorized by your depositor," followed by the account holder's typed name.[1]

24. Banks require that, before creating and depositing a demand draft, the originating merchant must have: (1) a consumer's bank routing number; (2) the consumer's bank account number; and (3) proof that the consumer authorized the transaction. The merchant or third-party payment processor then creates an electronic check in the name of the consumer and deposits it in the merchant's – or payment processor's – own bank account.

25. Prior to 2003, the payee was required to create a paper demand draft and physically deposit it at the payee's bank from which point it would enter the national check payment system. However, in an effort to reduce the burden of handling and maintaining paper copies of checks, in 2003, Congress passed The Check Clearing for the 21st Century Act ("Check 21 Act"). Pursuant to this statute, banks are permitted to process check transactions using electronic images of checks instead of the physical original (i.e., paper) check.

[1] Demand drafts are notorious in the banking industry and consumer protection community for their use as instruments of fraud. In 2005, in response to a request for public comment, America's Community Bankers, a prominent industry group that later merged with the American Banking Association, wrote to the Board of Governors of the Federal Reserve and the FDIC that "the number of unauthorized remotely-created demand drafts has become a significant problem" because of the "level of fraud and abuse associated with remotely created checks." That same year, the Attorneys General of 35 states jointly urged the Federal Reserve to eliminate such demand drafts, which are frequently "used to perpetrate fraud on consumers."

26. Because the financial transaction is premised on the transmission of a digital reproduction of a check, the depositor's bank can withdraw funds directly from a payor's bank account as if a paper check was used via the Federal Reserve Bank's check clearing system. Another consequence of the check-based nature of a Check 21 transaction is that when a consumer disputes a debit from his account, he must complete and sign an affidavit attesting that the withdrawal was unauthorized.

27. Due to the absence of a paper copy and the speed by which digital images can be processed between banks, fraudulent merchants working with third-party payment processors can exploit Check 21 Act processing to transfer money from a consumer's account without genuine authorization. An example of a Check 21 transaction between merchant, consumer, and banks proceeds as follows:

a. The merchant will obtain the consumer's bank account information, including the account number and bank routing number.

b. The payment processor will then generate a digital image file of a demand draft. The face of the demand draft purports that the draft has been created with the account holder's authorization.

c. The payment processor will send the demand draft digital image (or just the payment information contained in the digital image) to its own bank.

d. The payment processor's bank will transmit the demand draft digital image via the Federal Reserve Bank's check clearing system to the consumer's bank. Implicit in this transmission is the claim that the payor (i.e., consumer) authorized the payment to the merchant.

e. The consumer's bank withdraws money from the consumer's account and transmits that money through the banking system to the payment processor's bank.

f. The payment processor's bank credits the money into the payment processor's bank account.

g. The payment processor transmits the money from its own bank account to the merchant's bank account.

28. During this series of transactions, the third-party payment processor's bank receives fees from the third-party payment processor. The third-party payment processor receives fees from the merchant. And the merchant keeps whatever money remains from the amount withdrawn from the consumer's account.

29. Demand drafts are returned through the national banking system like all other checks. Some checks are immediately rejected by a consumer's bank for a variety of reasons: the account does not exist; the account is closed or frozen; the account owner has blocked checks to a certain payee; or there are insufficient funds to cover the check (referred to as "NSF"). In most instances, these kinds of returns are processed within one or two days. Other kinds of returns, including "unauthorized" and "breach of warranty" returns, can be returned over longer periods of time. These two categories of returns typically require the consumer to fill out an affidavit, signed under penalty of perjury, stating that he or she did not authorize the check.

30. Unlike other payment systems, such as credit card payments and Automated Clearing House (ACH) transactions, demand drafts are not monitored electronically by any supervisory authority. Therefore, a bank accepting large volumes of demand drafts for deposit must analyze rates of returned transactions for the demand drafts it submits into the national banking system, and consider those rates in the context of overall return rates for all checks processed though the

national banking system. According to the 2013 Federal Reserve Payments Study,[2] from 2009 through 2012, the annual rate at which checks were returned decreased from 0.5 percent to 0.3 percent. In other words, when CWB started working with the payment processor and merchants described below in 2012, the average rate of returned checks was *less than one-third of one percent*.

V.

THE SCHEME BY COMMERCEWEST BANK, A THIRD-PARTY PAYMENT PROCESSOR, AND FRAUDULENT MERCHANTS, TO DEFRAUD HUNDREDS OF THOUSANDS OF CONSUMERS

A. CommerceWest Bank Opens Accounts For A Third-Party Payment Processor Servicing Fraudulent Merchants.

31. In November 2011, a third-party payment processing company called V Internet Corp, LLC ("V Internet"), which was headquartered in Las Vegas, Nevada, approached CWB and asked whether the bank would open accounts for V Internet to process demand drafts on behalf of its merchants. V Internet was owned and controlled by an individual who resided in Las Vegas and Texas (hereinafter "V Internet Owner").

32. At the time it contacted CWB, V Internet operated under the name Altcharge. In addition to opening accounts under the name Altcharge, V Internet told CWB that it also wanted to open accounts for a new payment processing "brand," which it called Check Process.

33. CWB conducted due diligence of V Internet, including reviewing Altcharge's policies and its website. As a result of this review, CWB categorized the Altcharge business as "high risk." The Bank's due diligence file included pages from the Altcharge website stating that Altcharge specialized in the

[2] Available at https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.

creation and processing of demand drafts for merchants that had been prohibited from accepting other forms of payments, such as credit cards or ACH payments. For example, the website's "Frequently Asked Questions" section stated that Altcharge would process checks for "TMF Merchants," which refers to the "terminated merchant file," a list of merchants banned from processing credit card payments.

34. CWB did not conduct separate due diligence for V Internet's new "brand," Check Process. However, had CWB officials looked at the Check Process website, they would have seen that it included similar statements, stating "[i]n the world of merchant service providers, some businesses are considered more high risk than others. This doesn't mean these businesses can't obtain merchant accounts … If you want to accept checks for your business but are having trouble finding a processor Checkprocess.com may be able to help."

35. In December 2011, CWB opened accounts for both of V Internet's "brands," Altcharge and Check Process. On December 14, 2011, V Internet began depositing demand drafts (each of which represented a charge from the account of a consumer at another bank) into its CWB accounts. Two days later, CWB's primary contact with V Internet ("CWB Official No. 1") reported to CWB's CEO that "[w]e have hit gold with this relationship, it will be expanding. The founder, [V Internet Owner], would like to meet you and take you flying in his Russian fighter jet."

B. CommerceWest Bank Facilitated Over 1.3 Million Fraudulent Demand Drafts Involving V Internet And Two Fraudulent Merchants.

36. Initially, V Internet's business Altcharge processed payments for dozens of merchants. However, during the first six months of 2012, many of the merchants stopped processing payments through Altcharge. Some of Altcharge's largest merchants claimed that Altcharge wrongfully took money from the merchants' reserve accounts and refused to return it. CWB was aware of these

allegations. For example CWB's due diligence file contained printed pages of online complaints, in which a merchant alleged that Altcharge stole its money by wrongfully retaining funds in the merchants' reserve accounts.[3]

37. Thus, beginning in June 2012, nearly all of the transactions processed by V Internet were on behalf of just three merchants, each of which was engaged in a multi-million dollar consumer fraud scheme: YR Benefits, Loan Assistance, and a copycat of the Loan Assistance scheme that was run by V Internet Owner himself.

1. YR Benefits – A Telemarketing Scheme

38. From April 2012 through July 2012, CWB processed approximately 16,000 demand drafts, totaling approximately $7.4 million, on behalf of a group of telemarketing merchants, known to the bank as "YR Benefits." More than half (57%) of these were returned by consumers and consumers' banks.

39. In March 2012, V Internet approached CWB about a new merchant for which V Internet wanted to process payments using CWB accounts. V Internet explained that it had processed payments for the merchant in the past and that the merchant engaged in high-pressure telemarketing sales of discount medical plans. It stated that the merchant's business was high risk and that it would result in high return rates. It emphasized that the relationship would generate relatively large fees for both V Internet and CWB. V Internet proposed processing payments for YR Benefits through a separate account in the name of a joint venture between V Internet and the new merchant, rather than through V Internet's already-established accounts.

///

[3] CWB would also learn that one of Altcharge's largest merchants stopped processing demand drafts in April 2012 and sued Altcharge for stealing $1.4 million.

40. V Internet employees provided to CWB a written "Risk Management Proposal" and an Operating Agreement for the joint venture, referred to as "DLMLST." The managing members of the joint venture were the two principals of V Internet and another individual represented as a resident of British Columbia, Canada.

41. The DLMLST Risk Management Proposal provided to the Bank explicitly discussed the exorbitant return rates V Internet expected in the new account. Indeed, in light of the high number of returns that were expected, the Proposal established a reserve account[4] that would be required to have enough cash so that all returns would be covered (limiting the risk to CWB). In describing the mechanics of the reserve account, the Agreement included an example that assumed the merchant would generate a 50% return rate.

42. The Proposal also included provisions designed to separate the new business from the Bank's other accounts with V Internet. Specifically, V Internet requested that the Bank "acknowledge in agreement that this venture is completely separate from V Internet Corp LLC and any business from this deal should not affect same."

43. Finally, the proposal attempted to prohibit the Bank from contacting the new merchant, YR Benefits, stating "[w]e request in writing Commerce West to **not** have any direct deal [sic] with merchant . . . ." (emphasis in original).

44. V Internet employees also provided documentation relating to multiple telemarketing entities in connection with the proposed DLMLST/YR Benefits account. CWB's due diligence file for the YR Benefits account contained

[4] A reserve account is an account, separate from an operating account, which contains funds of a payment processor or merchant that are used to cover returns and bank fees. In the event a payment processor does not have enough money to pay returns or fees, the reserve account protects the bank from suffering a loss.

two telemarketing sales scripts, one touting an identity theft protection package and another a medical benefit discount card.

45. Despite these red flags, in April 2012 CWB permitted V Internet to open the accounts.

46. As predicted, the return rate for the YR Benefits account quickly increased to over 50%.

47. On July 13, 2012, CWB received explicit notice from another bank that it suspected YR Benefits was engaged in a fraud scheme targeting the elderly. In the letter, Zions National Bank ("Zions") alerted CWB to 100 unauthorized drafts presented to multiple Zions-affiliated banks and drawn on the accounts of elderly consumers. Many of the checks were demand drafts payable to YR Benefits. In stark terms, Zions said that it suspected CWB's customers were engaged in fraud:

> We are extremely concerned because 100% of the customers we have contacted regarding these items have indicated that the draft was not authorized, and the payee did not have permission to debit funds from any account. Of particular concern, we have found that the vast majority of the victims of these unauthorized drafts are elderly persons, prompting numerous elder abuse investigations at our banks . . . I trust that your institution has done proper due diligence in identifying the activities and sources of revenue for your customers who are depositing these drafts. I also trust that Commerce West will be filing a [Suspicious Activity Report] based on the high level of return items for these customers. (I feel pretty safe in assuming that my affiliate banks are not the only banks returning items as unauthorized).

48. On July 20, 2012, CWB terminated the DLMLST account. A CWB official explained the decision to V Internet, stating "[w]ith the return rate of the YR Benefits demand drafts running at 50% and the ratio of fraudulent/breach of warranty and demand letters to total returns running 98% of all returns, we cannot

continue to process for YR Benefits . . .” In other words, half of the checks deposited by YR Benefits into the CWB account were returned and nearly all of the returned checks were returned with affidavits from consumers indicating the checks were unauthorized.

49. CWB’s explanation continued: “*we have hit the radar with a number of major banks and it is now impacting CommerceWest financially* . . . we would not be able to defend our processing these items with so many returns for reasons other than [insufficient funds] to our regulators.” (emphasis added).

50. Thus, in choosing to terminate YR Benefits in July 2012, CWB acknowledged that high return rates (particularly when those returns were for reasons other than the account lacked sufficient funds) and complaints from other banks were red flags of fraud that the bank could not justify. Yet, as described more fully below, once CWB terminated YR Benefits, the overwhelming majority of V Internet’s processing activity came from just one other V Internet merchant. Like YR Benefits, this merchant was already generating approximately 50% returns, complaints from consumers and other banks, and other red flags. And yet despite its experience with YR Benefits, all of the other red flags about V Internet more generally, and strikingly similar red flags about V Internet’s one remaining merchant, CWB continued to permit V Internet to withdraw funds from consumer bank accounts.

2. Loan Assistance – A Payday Loan Finder Scam Involving Hundreds of Thousands Of Unauthorized Checks

51. From May 2012 through December 2012, CWB processed over 500,000 demand drafts totaling more than $15 million on behalf of a company called Loan Assistance. The business of Loan Assistance, purportedly, was to charge

consumers a $30 fee to help them find a payday loan.[5] Approximately 50% of the transactions were returned by consumers' banks.

52. V Internet did not notify CWB before it began depositing demand drafts for this new merchant, nor did it provide any due diligence or information about the merchant. When CWB officials realized that V Internet was processing large numbers of payments for Loan Assistance, the Bank conducted some basic due diligence and quickly found information indicating that Loan Assistance was committing fraud. On June 7, 2012, a CWB official found 483 complaints on a consumer complaint website called Scambook.com alleging fraud and unauthorized charges by Loan Assistance. These 483 complaints were entered over the course of just two months, between April 10, 2012 and June 7, 2012.

53. For example, one consumer stated "they debited my account $30.00 without any authorization. I don't even know who they are or how they got my banking information. Thet are just scam artist's [sic]."

54. Another consumer stated, "I checked my account. I don't even know this company. Took $30.00 from my account for a Cash Advance Fee, I never authorized. This is fraud and I will take it all the way to the top. It is hard enough to make ends meet and [then they] take people's money like this."

55. Consumer victims lodged hundreds of complaints against Loan Assistance with the Better Business Bureau and law enforcement agencies. On October 9, 2012, the Better Business Bureau issued a nationwide alert about Loan Assistance (and all of its alternate business names) warning consumers about unauthorized charges supposedly associated with online payday loans. According to the alert, as of October 9, all but one of the Loan Assistance business names had an "F" rating with the Better Business Bureau.

[5] Loan Assistance did not purport to provide the payday loans; only to help consumers find payday lenders.

56. Despite consumer complaints about fraudulent transactions, enormous return rates, and the other red flags described in Section C below,[6] CWB continued processing thousands of demand drafts every day for Loan Assistance through the end of 2012.

57. CWB never terminated Loan Assistance. Instead, in January 2013, the owner of V Internet informed CWB that he was taking over Loan Assistance's business model. CWB thus knowingly let the Loan Assistance scheme continue, but under a different name and with a different owner.

3. V Internet – Now Operating As Payment Processor And Merchant – Takes Over the Loan Assistance Scheme

58. On January 9, 2013, V Internet Owner informed CWB that he was taking over Loan Assistance's "business model." He told the Bank that he would run his own websites offering to help consumers find payday loans for a one-time fee of $30. He would then process those payments through his accounts at CWB.

59. From January 2013 through July 2013, V Internet – which was now acting as both the payment processor and the *sole* merchant – processed more than 750,000 demand drafts, totaling more than $22.5 million, through its accounts at CWB. As with the prior iteration of the scheme under Loan Assistance, approximately 50% of the checks were returned by consumers' banks.

---

[6] In August 2013, the Federal Trade Commission ("FTC") sued Loan Assistance, including its principals and all of its alternate business names. FTC v. Caprice Marketing, et al., Case No. 1:13-cv-06072 (N. D. Ill.). The FTC complaint alleged that consumers who went to Loan Assistance's websites were charged a $30 fee that they had not authorized and then Loan Assistance did not provide any service to help consumers find a payday loan. The complaint also alleged that many consumer victims never even went to any of Loan Assistance's websites – the company simply bought bulk lists of consumers' sensitive personal and financial information and charged a $30 fee to each bank account on the list.

60. Despite consistently high return rates, CWB allowed V Internet to deposit thousands of demand drafts nearly every day from January 9, 2013, through the end of the relationship in July 2013. In fact, in April 2013, CWB increased V Internet's daily deposit cap, which was the maximum number of demand drafts it allowed V Internet to deposit each day, from 4,900 demand drafts per day to 7,000 demand drafts per day.

61. As described in more detail below, by May 29, 2013, CWB finally researched the details of V Internet's processing patterns. CWB determined internally that V Internet was processing numerous $30 checks against each bank account and that all of the checks appeared to be fraudulent. However, even after making this determination, CWB did not terminate the V Internet accounts until July 15, 2013, after the Bank was told that the Department of Justice planned to seek an injunction under the Anti-Fraud Injunction Act.

C. CommerceWest Bank Knew Of, Or Was Deliberately Ignorant To, The Warning Signs Of The Schemes To Defraud Consumers As Described Above.

62. During the course of its relationship with V Internet, CWB was aware of major red flags indicating that V Internet and its merchants were engaged in consumer fraud, including abnormally high rates of returned checks, suspicious activity by the owner of V Internet, and explicit warnings from consumers' banks that V Internet's merchants appeared to be engaged in fraud.

1. CommerceWest Bank Continued Processing Demand Drafts Despite Incredibly High Return Rates.

63. The banking industry is aware that high rates of returned transactions – regardless of the specific reason for the return – indicate suspicious activity. For example, the U.S. Financial Crimes Enforcement Network has stated:

> *Fraud:* High numbers of consumer complaints about Payment Processors and/or merchant clients, and particularly **high numbers of returns or chargebacks**

> **(aggregate or otherwise)**, suggest that the originating merchant may be engaged in unfair or deceptive practices or fraud, including using consumers' account information to create unauthorized RCCs or ACH debits.

FinCEN Advisory: Risk Associated with Third-Party Payment Processors, FIN-1012-A010 (October 22, 2012) (emphasis added).

64. From April 2012 through July 2013, CWB knew that V Internet's three primary merchants experienced abnormally high return rates – the percentage of transactions that are reversed – which CWB also knew is a primary indicator of consumer fraud. During that time period, approximately 50% of the checks deposited by V Internet were returned – a return rate more than 150 times greater than the national average for returned checks.

65. Moreover, many of these returns included explicit evidence that consumers denied authorizing the transactions. More than 100,000 of V Internet's demand drafts were returned as "unauthorized" or "breach of warranty." Many of these returns included affidavits from consumers stating that they did not authorize the transaction.

66. As discussed above, prior to the start of processing, V Internet and YR Benefits informed the Bank that they expected YR Benefits to generate 50% returns. Nevertheless, CWB opened accounts for DLMLST/YR Benefits. As predicted, the returns quickly exploded to just over 50% of all transactions. When it terminated YR Benefits, the Bank cited the high return rates as the primary reason it could not continue to accept demand drafts from YR Benefits. However, over the next 12 months, the Loan Assistance scheme and the V Internet iteration of the Loan Assistance scheme generated similar return rates.

67. CWB employees monitored return rates of V Internet's merchants. They monitored total returns, as well as each of the return reasons associated with demand draft returns. Bank employees considered some return reasons, including Altered/Fictitious Account, Not Authorized, and Warranty

Breach, to be particularly problematic and indicative of fraud. For example, on June 25, 2012, a CWB employee emailed Bank Official No. 1 a chart reflecting daily return rates for "problematic items (Altered Fictitious/ Not Authorized/ Warranty Breach)." The employee characterized the chart as showing a downward trend of these problematic categories of returns. Nevertheless, the chart showed daily return rates of these "problematic" return reasons between 15% and 35% for nearly every day in June. The employee then expressed his skepticism that V Internet and its merchants would meaningfully decrease return rates, remarking "[a]ccording to this, we should be down to 0% by August. Ha!"

68. V Internet's consistently high returns caused CWB to dedicate huge numbers of employee hours to processing returns. CWB did not have an automated way to process and track the thousands of returned demand drafts it was receiving every day. Instead, CWB employees viewed images of returned checks on a computer, clicked a button to return the funds, and then manually entered the check information into a database. As return volumes exploded in the summer of 2012, CWB instructed employees of its Operations Department to spend all of their time processing returned demand drafts related to V Internet. Employees worked overtime and on weekends to keep up with the return volume. When employees still could not keep up with the volume, CWB hired temporary employees for the sole purpose of processing V Internet's returned demand drafts.

69. In September 2012, after more than three months of persistently high returns by Loan Assistance, CWB officials began to worry that Loan Assistance would not have enough money in its account to cover the returns and pay CWB's fees. On September 14, 2012, CWB Official No. 1 emailed V Internet: "There are two options for [Loan Assistance]; one is a reserve account of $500,000

and the other would be to go to eSignature.[7] I am good with either of these options. We need one or the other in place by month end." Thus, CWB gave V Internet and Loan Assistance a choice of providing electronic evidence that a consumer had actually authorized the check or simply creating a reserve account to protect CWB.

70. CWB Official No. 1 then acknowledged the difficulty V Internet would have finding another bank willing to have V Internet's merchant, Loan Assistance, as a customer: "**No other bank that understands 3rd party processing will bank them without a reserve and if they find a bank that will then it will only be a matter of time before they will be asked to leave due to the return volume**." (emphasis added).

71. Despite additional inquiries from CWB, neither Loan Assistance nor V Internet ever implemented eSignature.

72. By November 2012, V Internet was unable to pay all of the fees it owed CWB and it developed a significant overdraft in its accounts. After returning approximately 50% of the demand drafts it deposited, and paying a return fee to CWB on every returned check, there was no money left in V Internet's accounts. Moreover, CWB had not created a sufficient reserve account to ensure that its fees were paid. By the end of November 2012, the overdraft had grown to approximately $1.5 million. Rather than terminating V Internet at this point, CWB worked with V Internet to restructure the accounts so CWB could recoup the fees V Internet owed. CWB created multiple reserve accounts to pay down the accumulated overdraft and ensure that CWB received its fees in the future.

[7] ESignature is a consumer's electronic signature, typically created using a computer mouse at the time of an Internet-based debit authorization. The suggested addition of eSignature to Loan Assistance's demand drafts was intended to increase assurance that consumers had authorized the transactions reflected on the demand drafts.

73. CWB also agreed to reduce its per-item return fee from $12 to $6, which increased the profit potential for V Internet and Loan Assistance even though the return rates remained incredibly high. The vast majority of the fees earned by CWB during to its relationship with V Internet were due to returned transactions. CWB charged V Internet a fee on each returned item. Such a fee can serve as a deterrent to discourage a payment processor from working with merchants that generate large numbers of returned items and to incentivize legitimate merchants to lower return rates. However, because CWB did not terminate V Internet despite consistently high return rates, the returned item fees did not serve as a deterrent to fraud. Instead, the fees generated millions of dollars for the Bank's bottom line.

74. In January 2013, when V Internet took over Loan Assistance's business model and thereby became the merchant, CWB officials expressed concerns about erratic return patterns. However, as they had done throughout the relationship, CWB officials asked questions about V Internet's extremely high return rates, while allowing it to continue processing. On January 22, CWB Official No. 1 emailed CWB's CEO to inform him "we were hit with almost 12,000 returns . . . something is not right with the way [V Internet Owner] is processing." On February 11, CWB Official No. 1 emailed the CEO to report another inexplicable spike in returns, with a large number of returns with the reason "Account Closed." The CEO responded "I am concern [sic] that we at CWB cannot figure out what the returns were related [to]." Three days later, on February 14, CWB Official No. 1 emailed the CEO with "GREAT news" that V Internet's returns decreased slightly and "[i]f this keeps up we will get the return ratio down into the 50 percentile."

75. Beginning in January 2013 and continuing through July 2013, CWB sent V Internet regular emails informing V Internet of its return rate and asking V Internet to work to reduce the rate. For example, on February 1, 2013,

CWB Official No. 1 emailed V Internet Owner, stating: "Our overall return to deposit ratio for the month of January 2013 was 61%. Our goal needs to get this down to 40% with the ultimate goal to 30%." These emails provided constant reminders to both CWB and V Internet of the consistent, egregious return rates, while stating lower, albeit still extraordinarily high, target return rates that were never met.

2. CommerceWest Bank Knew About Allegations That V Internet's Owner Had Stolen Money By Knowingly Submitting Thousands Of Duplicate Checks.

76. In November 2012, CWB learned that V Internet had, on two separate occasions, submitted a daily file of demand drafts twice, effectively double-billing consumer accounts.

77. On November 21, 2012, a former V Internet official, who had left the company in September, emailed CWB Official No. 1, stating that he had learned that V Internet Owner had twice re-named a daily batch of demand drafts and re-submitted both batches for processing. CWB determined that on November 14, 2012, V Internet re-submitted the entire daily deposit from November 5, 2012. On November 19, 2012, V Internet re-submitted the entire daily deposit from October 30, 2012. Thus, consumers whose accounts were debited on those days were debited twice. Processing of these duplicate daily files resulted in $576,195.23 in duplicate charges against more than 19,000 individual consumer accounts.

78. On November 23, 2012, CWB Official No. 1 emailed V Internet Owner to ask about the duplicate file issue. She stated "you can understand how this looks so I am hoping that there is a good explanation." V Internet Owner denied that he intentionally re-submitted the daily batch files and blamed the duplicate deposits on computer errors.

79. On November 24, 2012, a V Internet official (hereinafter referred to as "V Internet Official No. 1") called CWB Official No. 1 and described the duplicate file issue. After this phone call, V Internet Official No. 1 sent multiple text messages asking CWB Official No. 1 to arrange a meeting with CWB's CEO to discuss what V Internet Official No. 1 believed to be V Internet Owner's intentional processing of the two duplicate files. CWB officials did not arrange a meeting with V Internet Official No. 1. Two days later, V Internet Official No. 1 informed CWB that he was resigning from V Internet.

80. Even though two V Internet officials – one former and one current – contacted the bank and disclosed that V Internet Owner had intentionally re-submitted thousands of demand drafts, thereby attempting more than $500,000 in unauthorized debits from consumer bank accounts, CWB continued processing for V Internet.

3. CommerceWest Bank Received Explicit Notice From Consumers And Consumers' Banks, Indicating That V Internet Was Processing Unauthorized Debits Against Consumers' Accounts.

81. Beginning in late June 2012, consumers' banks began contacting CWB regarding large numbers of unauthorized $30 demand drafts being debited against the bank's customers. Many of the banks were sending affidavits from their customers stating, under penalty of perjury, that the $30 check was not authorized. Along with these fraud affidavits, some of the banks stated that they believed CWB's merchant was engaged in fraud and warned CWB, often in blunt terms, about the consequences of facilitating fraudulent schemes.

82. Beginning with a June 28 letter from Bank of America, described below, CWB developed a practice of instructing V Internet to block the routing numbers of complaining banks – thereby not allowing any checks to be debited against customers of those complaining banks – while allowing the charges to continue against customers of all other banks. These letters served as explicit

notice that other banks suspected that V Internet and its merchants were engaged in fraud, while further highlighting the large number of consumers who denied authorizing the demand drafts. And yet, CWB blocked charges only against consumers at the complaining banks while allowing V Internet and its merchants to continue charging consumers of all other banks.

83. On June 28, 2012, CWB received a letter from Bank of America regarding unauthorized $30 demand drafts debited against Bank of America's customers. The letter stated: "Since May 1, 2012, over 1200 Bank of America accounts have been debited in the amount of $30, via demand draft by your customer identified above. Our customers are advising us that these transactions were not authorized. These transactions occur daily." (emphasis in original). CWB knew that these transactions related to Loan Assistance because it was the only merchant depositing large volumes of $30 checks. The letter provides explicit warning to CWB that it may be facilitating a massive consumer fraud scheme:

> This letter is to put CommerceWest Bank on notice that Bank of America will pursue all of its rights against Commerce West with regard to any and all unauthorized transactions . . . I am sure you are aware of the recent consent order from the [OCC] against Wachovia Bank with regard to unauthorized remotely created checks Wachovia accepted for deposit from payment processors and telemarketers. The cost to Wachovia is approximately $144 million. This situation serves as a cautionary tale for all financial institutions that accept deposits from telemarketers with high rates of returned items.[8]

[8] In 2010, the United States prosecuted Wachovia Bank for criminal violations of the Bank Secrecy Act. See United States v. Wachovia Bank, NA, Criminal Action No. 10-10265 (S.D. Fla.). As noted by Bank of America in its letter, some of the allegations against Wachovia arose from its relationships with four different third-party payment processors and their fraudulent merchants. Wachovia also settled private class action litigation and an enforcement action by the Office of the Comptroller of the Currency arising from the same activity. These matters were

84. On July 5, 2012, CWB Official No. 1 had a conversation with a representative of the Bank of America Check Fraud Claims Department. CWB agreed to block all Bank of America routing numbers so that Loan Assistance would not be able to process checks against Bank of America customers' accounts. CWB Official No. 1 then emailed V Internet and requested that they block all Bank of America routing numbers. Because V Internet created the demand drafts on behalf of its merchants and transmitted them to CWB in a single, daily file, CWB relied on V Internet to block the routing number and to ensure that it did not deposit additional demand drafts drawn on Bank of America accounts.

85. Thus, after two months of processing checks for Loan Assistance, another bank – one of the largest banks in the country – alerted CWB that Loan Assistance had deposited over one thousand unauthorized checks from consumer bank accounts. Even though CWB had agreed to protect Bank of America's customers by blocking Bank of America routing numbers, CWB continued to process thousands of demand drafts every day against consumers with accounts at other banks.

86. On August 14, 2012, CWB received a letter from a Financial Crimes Manager at Wells Fargo complaining about unauthorized demand drafts against Wells Fargo accounts. The letter stated that Wells Fargo customers "claim that draft(s) having paid through their accounts were unauthorized and that no permission or authority was given for the charge to be processed against their account . . . . Wells Fargo has received complaints/claims from a substantial number of clients. Claims during the last 60 days exceed 2000." The letter then references the regulatory guidance about fraud risks associated with third-party payment processors, stating "[t]his activity appears to be possibly related to OCC

---

resolved by Wachovia agreeing to pay up to $160 million in restitution to consumers, a $10 million fine to the U.S. Treasury, a $9 million payment to independent consumer protection education programs, and other conditions.

Bulletin 2008-12, issued April 24, 2008, as well as FDIC FIL-3-2012, issued January 31, 2012."

87. On September 7, 2012, CWB Official No. 1 responded to Wells Fargo, stating "[a]fter receipt of your letter we opened an investigation of the items in question as well as discontinued processing of all items during the investigation period. Our investigation is now closed. [Neither] Wells Fargo nor any Wells Fargo clients will be receiving any further paper demand drafts from this merchant."

88. Once again, CWB instructed V Internet to block the routing numbers of one of the country's largest banks after it complained of unauthorized checks connected to Loan Assistance. Rather than terminating the merchant that was generating thousands of complaints of fraud and unauthorized charges, CWB continued to process checks against the accounts of consumers with accounts at other banks.

89. But this was not the end of the complaints. CWB continued to receive complaints from consumers' banks relating to unauthorized charges by V Internet and its merchants. When banks asked to have their routing numbers blocked, CWB agreed and instructed V Internet to add that bank to the growing list of blacklisted routing numbers.

90. By November 2012, CWB had tasked a low-level employee in the Operations Department with fielding calls from complaining banks. On November 19, 2012, the employee emailed her supervisors to alert them that multiple banks had called to complain about demand drafts that had been presented with fictitious account numbers. She wrote: "I have received calls from 3 different banks regarding Fictitious Account Numbers. They are calling us to let us know that they suspect Fraud from the Depositor, as the account numbers on the remotely created checks or makers do not exist."

91. On November 23, 2012, another bank sent a fax to the CWB employee disputing four checks. The consumers' bank also included a printed page

of complaints the bank had found online, on which an employee of the consumer's bank had written "Recent Nov online complaints!"

92. On December 11, 2012, after CWB requested that V Internet block yet another bank routing number, a CWB supervisor emailed employees in the Operations Department, stating "hopefully this will help minimize our daily processing. Please continue monitoring any suspicious issues **when time allows**, do not spend extra time trying to resolve fraudulent cases, remember that we have to focus on processing first." (emphasis in original). CWB chose to devote its resources to processing the astounding number of returns generated by Loan Assistance – which also generated substantial fee income for the bank.

93. In January and February of 2013, after V Internet took over the Loan Assistance scheme, it processed thousands of checks against accounts at banks that had previously asked to have their routing numbers blocked from receiving any checks from V Internet. In an email dated February 11, 2013, CWB Official No. 1 told V Internet Owner she had received "communication from the Financial Crimes Manager of Wells Fargo due to over 2,800 items hitting their bank against closed accounts." On February 19, 2013, CWB Official No. 1 forwarded V Internet Owner an email in which Bank of America was claiming it was "still seeing fraud claims for drafts" created by V Internet.

94. These renewed complaints provided CWB with evidence that V Internet had removed internal blocks that had prevented debits against accounts of two banks that had insisted their routing numbers be blocked. Additionally, the renewed complaint from Wells Fargo indicated it had received 2,800 demand drafts drawn on closed accounts. CWB knew that "closed account" returns were a red flag of fraud. Indeed, on February 25, 2013, CWB Official No. 1 emailed V Internet Owner to alert him that returns for the reasons "Unable to Locate Account" and "Closed Account" had increased substantially. "The erroneous account numbers and closed accounts are the problem since these are two of the reason codes

that indicate potential fraud." And yet, CWB again instructed V Internet only to block the Wells Fargo and Bank of America routing numbers and continued processing its demand drafts.

95. On May 24, 2013, CWB received a large shipment from TD Bank, consisting of four boxes full of consumer affidavits stating that V Internet demand drafts were unauthorized. A senior CWB Official (hereinafter "CWB Official No. 2") sent an email to CWB Official No. 1, attaching a picture of the boxes of affidavits, and stated "Not sure how we are going to get these all processed. My bigger concern is what the heck is he doing (something is very wrong)."

96. CWB Official No. 2 then researched V Internet's transactions and determined that they were processing multiple demand drafts against each consumer's bank account. This "research" consisted of a CWB official checking CWB's own system to determine how V Internet was charging consumers' accounts. CWB could have done this simple research at any time to determine why its merchant was generating complaints and abnormally high return rates. In other words, CWB only needed to examine its own records to detect and understand the fraud being perpetrated by its merchant.

97. On May 29, 2013, CWB Official No. 2 sent an email to CWB Official No. 1 and the Bank's CEO, stating "I have findings that are very very concerning." She explained that she researched unauthorized claims from the TD Bank affidavits, as well as randomly selected account numbers. For each account number she researched, she found that V Internet had processed between three and eight demand drafts. "I did not find one account of all I selected to search that was only processed once." The significance of these systemic, repeat charges led CWB Official No. 2 to a clear conclusion: "All the transactions at this point appear to be fraudulent and it is a matter of time until we receive many more breach of warranty claims, unauthorized transaction claims, as well as subpoena's [sic] from government agencies and police."

D. Even After Determining that V Internet Was Processing Unauthorized, Fraudulent Transactions, CommerceWest Bank Processed Its Demand Drafts For Six More Weeks

98. As of May 29, 2013, CWB Official No. 2 had determined that all of V Internet's demand drafts were fraudulent, duplicate charges against consumers' bank accounts. She summarized her findings in an email to CWB Official No. 1 and CWB's CEO. And yet, incredibly, rather than immediately terminating V Internet's accounts, CWB allowed V Internet to continue processing for more than six additional weeks (and would have continued beyond that, had the Department of Justice not intervened). During that time period, V Internet deposited 199,816 additional fraudulent demand drafts, totaling approximately $6 million.

99. In keeping with their standard practice, CWB asked V Internet to block the TD Bank routing number – protecting TD Bank customers from additional fraudulent charges, but allowing other demand drafts against customers of other banks to continue. CWB asked V Internet to explain the duplicate charges and provide documentation showing authorization for the demand drafts. For more than one month, CWB asked V Internet to provide full authorizations for each of the disputed charges against TD Bank customers. On multiple occasions, V Internet provided information that CWB officials did not think constituted proof of authorization. CWB continued to accept V Internet's fraudulent demand drafts throughout this time period.

100. In early July 2013, CWB notified the U.S. Department of Justice, from whom it had received a subpoena requesting documents relating to its potential facilitation of consumer fraud, that it had decided to terminate V Internet's accounts. CWB stated that it would allow 30 days for V Internet to wind down its processing activity. On July 12, 2013, the Department of Justice notified CWB that it planned to seek an immediate injunction under the Anti-Fraud Injunction Act, 18 U.S.C. § 1345, in order to prevent CWB from continuing to process demand drafts on behalf of V Internet. On July 15, 2013, CWB finally notified V Internet that CWB would

no longer accept its demand drafts and that CWB would be terminating all of V Internet's accounts.

101. Between April 2012 and July 2013, CWB processed more than 1.3 million demand drafts, totaling more than $45 million in funds withdrawn – or attempted to be withdrawn – from consumer bank accounts, for V Internet and its merchants.

102. In exchange, CWB generated over $5 million in fees, including approximately $4.29 million after July 2012. The fees CWB generated from its relationship with V Internet were an important source of revenue. In 2012, CWB earned more than $2.9 million in gross fees from V Internet and reported a bank-wide profit of $4.2 million. In the first half of 2013, CWB earned nearly $2.2 million in gross fees from V Internet and reported a bank-wide profit of $2.9 million.

COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

103. The United States incorporates by reference paragraphs 1 through 102 as if fully set forth in this paragraph.

104. CWB violated the Wire Fraud statute, 18 U.S.C. §1343, by participating in a scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses with the intent to defraud, using wire communication and there is a substantial likelihood of future violations.

105. CWB's conduct constitutes or is likely to constitute a continuing and substantial injury to the United States and its citizens. Absent injunctive relief, CWB's conduct presents a reasonable likelihood or a cognizable danger of recurrence.

106. The United States seeks, pursuant to 18 U.S.C. § 1345(b), a permanent injunction restraining all future fraudulent conduct and any other action that the Court deems just in order to prevent a continuing and substantial injury to the persons and entities affected by the Defendant's fraudulent scheme.

COUNT II

(12 U.S.C. § 1833a – Civil Penalties)

107. The United States incorporates by reference paragraphs 1 through 102 as if fully set forth in this paragraph.

108. CWB violated the Wire Fraud statute, 18 U.S.C. §1343, by participating in a scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses with the intent to defraud, using wire communication.

109. This wire fraud scheme affected numerous federally-insured financial institutions, including the banks of the consumer victims from whom money was taken without authorization, and CWB itself.

110. Accordingly, CommerceWest Bank is liable to the United States for civil penalties as authorized under 12 U.S.C. § 1833a(b).

///

WHEREFORE, the United States requests judgment against Defendant, as follows:

a. An injunction under 18 U.S.C. § 1345 enjoining Defendant from processing financial transactions for third-party payment processors when it knows or is deliberately ignorant that the transactions facilitate consumer fraud;

b. A judgment imposing a civil penalty against Defendant up to the maximum amount allowed by law; and

///

c. Such further relief, including but not limited to equitable relief under the Court's inherent powers, as the Court deems just.

DATED: March 10, 2015

Respectfully,

BENJAMIN C. MIZER
Acting Assistant Attorney General
JONATHAN F. OLIN
Deputy Assistant Attorney General
Civil Division

MICHAEL S. BLUME
Director
RICHARD GOLDBERG
Assistant Director
Consumer Protection Branch

//s// John W. Burke

JOHN W. BURKE
Trial Attorney
Consumer Protection Branch

STEPHANIE K. YONEKURA
Acting United States Attorney
LEON W. WEIDMAN
Assistant United States Attorney
Chief, Civil Division

//s// Anoiel Khorshid

ANOIEL KHORSHID
Assistant United States Attorney

Attorneys for Plaintiff United States of America

DEMAND FOR JURY TRIAL

Plaintiff United States of America hereby demands a trial by jury.

DATED: March 10, 2015

Respectfully,

BENJAMIN C. MIZER
Acting Assistant Attorney General
JONATHAN F. OLIN
Deputy Assistant Attorney General
Civil Division

MICHAEL S. BLUME
Director
RICHARD GOLDBERG
Assistant Director
Consumer Protection Branch

//s// John W. Burke

JOHN W. BURKE
Trial Attorney
Consumer Protection Branch

STEPHANIE K. YONEKURA
Acting United States Attorney
LEON W. WEIDMAN
Assistant United States Attorney
Chief, Civil Division

//s// Anoiel Khorshid

ANOIEL KHORSHID
Assistant United States Attorney

Attorneys for Plaintiff United States of America